Pannonia Bio Zrt.

PRIVACY POLICY

DATA PROCESSING REGARDING THE OPERATION OF THE HTTPS://PANNONIABIO.COM/HU/ WEBSITE

1. GENERAL INFORMATION

Data Controller: Pannonia Bio Zrt. (registered office: 1051 Budapest Zrínyi utca 16. I/I, Hungary).

The Data Controller's data processing principles are in compliance with the applicable legislation on data protection, in particular:

- The Constitution of Hungary (Freedom and Responsibility, Article VI);
- Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation) - ("GDPR")
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information - ("Info Code.");
- Act V of 2013 on the Civil Code - ("Civil Code");
- Act I of 2012 on the Labour Code - ("Labour Code").

Data Subject: Data Subject shall mean the visitor of Data Controller's website (https://pannoniabio.com; hereinafter: "**Website**").

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

1.1. The purpose of this Privacy Policy is to supply essential information to the Data Subject about the data processing the Data Controller performs with respect to all the relevant data protection regulations.

1.2. The Data Controller is committed to the protection of the Data Subject's personal data and particularly wishes to observe the Data Subject's fundamental right to informational self-determination.

1.3. The Data Controller reserves the right to alter this Privacy Policy and commits to supply information about any such alteration in accordance with the relevant legal regulations as effective.

1.4. Data Controller:

a) processes the personal data lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');
b) collects personal data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**');
c) processes personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
d) processes accurate and up to date data ('**accuracy**');
e) keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('**storage limitation**');
f) processes the personal data in a manner that ensures appropriate security of the personal data ('**integrity and confidentiality**').

1.5. Should you have any question regarding the Privacy Policy or the Data Controller's data processing regarding the Website, please contact our colleague on the following email address: info@pannoniabio.com.

2. DATA PROCESSING

The Data Controller strives to limit its personal data processing activity to what is absolutely necessary. Nonetheless, the processing of some personal data is inevitable. The Data Controller processes the personal data generated during the visit of the Website.

2.1. "Career" and other employment related contact

Purpose of the data processing: to recruit and hire employees. The Data Subject's personal data is necessary to examine whether the Data Subject is suitable for the position he/she applied to, in addition, the Data Controller needs the Data Subject's contact details to reach the Data Subject in connection with the Data Subject's application.

Legal basis of the data processing: The basis of the data processing is the Data Subject' consent (GDPR Article 6 Section (1) point (a)). By submitting the Data Subject's application to a position that the Data Controller advertises, the Data Subject consents to the use of his/her personal data in connection with the recruitment process which includes in particular the application, interviewing the candidate and, if successful, making an offer to the Data Subject.

Should the employment relationship not be concluded between the Data Subject and the Data Controller, Data Subject unequivocally and expressly declares that he/she has read the present privacy policy and gives consent to Data Controller to process his/her personal data provided in the course of the application for the relevant position. In this case the legal basis of processing personal data is the consent of the Data Subject (GDPR Article 6 Section (1) point (a)). In this manner Data Subject gives consent to the Data controller to process the personal data provided by storing it in the Data Controller's talent pool – even after the event of an unsuccessful application – and to contact the Data Subject if a position opens up, for which the Data Subject might have the necessary experience and/or qualifications.

List of the processed personal data: The Data Controller only processes personal data that the Data Subject provides when applying for the position including:

- Name;
- Contact details (e-mail address phone number etc.)
- Educational background and professional experience and skills in the form of curricula vitae.
- Other personal data provided for the purpose of applying for a job
- Certificate of good conduct

Source of the processed data: The Data Controller obtains personal data from:

- the Data Subject
- public online recruitment databases or by the transmission of data by recruiters or recruitment companies,
- transfer by third parties (employees)

Duration of data processing: the Data Controller will process personal data for as long as the above purpose is fulfilled. If the Data Subject is successful as an applicant and an employment relationship is concluded with the Data Subject, Data Controller shall process the Data Subject's personal data until it is required for the purpose of the employment.
In case the Data Subject gave consent to the Data Controller to process his/her curricula vitae even if the application was unsuccessful, then Data Controller processes the personal data for 2 years or until the Data Subject revokes their consent given.

Place of data processing: the Data Controller stores the personal data at its own servers located at its headquarters and at Airtable's servers (business entity name: Formagrid Inc; registered office: 799 Market St Ste 8, San Francisco, CA 94103)

Persons having access to the personal data: personal data is processed by the HR department of the Data Controller. During the recruitment procedure, the right to access the personal data of the Data Subjects is granted to the managerial employees who have the right to decide on the position advertised. The Company will not transfer the Data Subjects' personal data to third parties, unless it is legally obliged or authorized to do so.

2.2. Data processing in relation to health status

Purpose of the data processing: ensuring food safety and the smooth operation of the food production activities carried out by the Data Controller. The Data Controller needs the data provided by the data subject to identify the data subject and to verify their health status and compliance with the minimum personal hygiene requirements laid down in food safety legislation.

Legal basis of the data processing: The legal basis for data processing is the legitimate interest of the Data Controller (GDPR Article 6(1)(f) in accordance with GDPR Article 9(2)(g)). The data subject acknowledges that the Data Controller has a legitimate interest in ensuring food safety and therefore it is essential to verify that persons entering the food production facility are in a suitable state of health and hygiene. It is also in the legitimate interest of the Data Controller to do everything possible to prevent contamination of the food chain, which could result in the illness of a number of individuals and significant damage to the Data Controller's reputation.

List of the processed personal data: The Data Controller shall only process personal data provided by the Data Subject in the health declaration required prior to entering the food production area:

- Name
- Date of birth
- Company/employer name
- Start date of activity
- Statement on health status made in the health declaration in connection with the above
- Statement on contagious diseases made in the health declaration in connection with the above
- Statement in the health declaration regarding wounds and bandages in connection with the above

Source of the processed data: The Data Controller obtains personal data from the Data Subjects:

- Via an online form completed prior to admission; or
- Via a paper-based form completed prior to admission.

Duration of data processing: The Data Controller shall process personal data until the above purpose is fulfilled, but for a maximum period of 1 year. After 1 year, in the event of a new entry, the Data Controller's subcontractors and their employees are required to complete the declaration again so that the Data Controller always has up-to-date data.

Place of data processing: Personal data provided on paper-based forms is primarily processed at the reception desk and in the security room at the time of entry, and the forms are stored in a locked cabinet next to the reception desk. In the case of online forms, the Data Controller stores the personal data processed on the servers of Microsoft Ireland Operations Limited (registered office: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland), which provides the Microsoft Forms services.

Persons having access to the personal data: The Data Controller's security department and reception staff may access the personal data provided in connection with access control. In addition, the Data Controller's environmental, health and safety (EHS) staff, as well as information technology (IT) and quality assurance (QA) employees may also encounter personal data to the extent necessary to perform their duties, i.e., in connection with updating, maintaining, and editing online forms. Reception staff may also have access to the data in order to perform their administrative duties.

2.3. Data processing regarding “Cookies”

The use of the website does not generally require the collection of any personal data. The Data Controller may collect certain data when you browse the website in order to ensure the smooth operation of the website, improve the services available, prevent possible abuse, measure traffic, improve the user experience and perform statistical analysis. This data collection may in some cases involve the processing of personal data.

Cookies (HTTP cookies) are small data files that a website operator places on a user's device during the use of a website. These data files are saved and stored by the visitor's web browser. Cookies enable the website operator to identify the user on subsequent visits, distinguish the user from other visitors and provide customised information and content through the browser.

When visiting the website, or at any time thereafter, the Data Subject has the possibility to change the information about the storage of cookies in the cookie banner (cookie manager) on the website. The Data Subject also has the possibility to change the settings for certain cookies via his/her browser.

Cookies have multiple functions and can be used for various purposes, such as:

- **necessary cookies**: their use is essential for navigating the Website and for the operation of the Website. Without them, the Website or parts of the Website may not function properly or at all.
- **functional cookies:** the purpose of these cookies is to improve the user experience e.g. by remembering the device the user used for browsing, the language settings, the custom settings;
- **statistics cookies:** statistic cookies are collected anonymously; they help to understand how visitors interact with the Website;
- **marketing cookies:** these cookies collect detailed information about the user's browsing habits and are used to deliver advertised content to the user. These cookies are placed on the Website by third party service providers.

In the case of cookies of the first category (necessary cookies), it is sufficient for the website operator to inform the Data Subject in advance of the placement and functioning of the cookies that will be installed on the Data Subject's device during the use of the website. In contrast, for the use of cookies in the second, third and fourth categories, the website operator must obtain the Data Subject's explicit consent in advance. This consent can be given by the visitor through the cookie management interface of the website.

Purpose of data processing: We use cookies on our website to ensure the proper functioning of the site, including the accessibility of available features and services, to facilitate browsing and to improve the user experience by storing your preferences and visit history. Cookies also contribute to providing visitors with a high level of service, enhancing the security of the browsing process and improving our services by providing data and statistics about the use of the Website. In the case of third-party cookies, this information is also available to the third party concerned. By re-reading cookies previously placed on the device, it is possible to link a particular browsing session to previous visits, thus allowing us to carry out a deeper analysis of browsing habits. These analyses allow us to provide a personalised user experience, while preserving anonymity, and to display targeted advertising and marketing messages.

Legal basis for processing: the legal basis for our data processing in relation to cookies is the consent of the Data Subject (Article 6 Section (1) point (a) GDPR). The exception to this is cookies that are essential for the proper functioning of the site, in which case the processing is based on Article 6 Section (1) point (f) GDPR, i.e. legitimate interest. The Data Controller has a legitimate interest in the proper functioning of the website and the services provided on it.

Duration of data processing: some of the cookies used are valid only for the duration of the browsing session and are intended for the secure processing of data. These short- term cookies are automatically deleted after closing the browser. In addition, there are also longer-lasting persistent cookies which remain on the device to facilitate re-use of the site. These are stored for a pre-defined period of time and usually expire after a few days. They can, of course, be removed by the Data Subject at any time in the browser settings if necessary. Persistent cookies

are not automatically deleted when the browser is closed, but remain active until they reach their expiry date or are manually deleted.

Scope of data processing: by using cookies and reading them back, we process the website usage and browsing data of Data Subjects and related information.

The Data Subject may reject cookies on his or her computer or other browsing devices, or in the settings of the web browser (typically under Device / Settings / Privacy / Cookies) that the Data Subject uses to access the Website. If cookies are rejected, the Data Subject will not be able to take full advantage of the features and services of the Website and, as a consequence, the Data Controller cannot guarantee full, smooth and uninterrupted use of the Website.

Data Controller uses the following cookies:

Function	Name	Purpose	Expiry
statistics cookies	_ga_JEHXNQPJ0B	Web analytics support, user differentiation, website performance measurement and improvement.	2 years
statistics cookies	_ga	Statistical analysis, visitor tracking.	2 years
functional cookies	_cfuvid	Identification of user sessions, filtering of malicious attacks.	30 minutes or the end of the session.
functional cookies	fs-cc	Records the user's consent or rejection of cookies.	6 months.

Some cookies are set by external services and

- are under the control of the third-party service, not the Data Controller;
- can be accessed on any website that makes use of the service;
- can be used to track a user from one site to another;
- enable Data Contoller to deliver more relevant advertising to users.

2.4. The Data Controller does not use automated decision-making, including profiling.

3. OTHER DATA PROCESSING

3.1. The Data Controller may occasionally perform other personal data processing. Information about any data processing not mentioned in this Privacy Policy will be supplied on the data collection.

3.2. The Data Subject is informed that the court, the public prosecutor, the criminal investigation authority, the infringements authority, the relevant data protection authority, as well as other authorities authorized by legal regulation may request information, data and documents from the Data Controller, who will grant such requests to the extent it is required by the relevant legal regulations. The Data Controller will disclose personal data to the authorities only to the extent it is indispensable for the fulfilment of the authorities' meticulously detailed request for information as regards the scope and purpose of information.

4. DATA PROCESSORS

4.1. The Data Controller assigns the following data processors during its data processing activity:

Webflow Inc. (registered office: 398 11TH St FL 2 San Francisco, CA, 94103-4393 United States): a private company incorporated under the laws of the United States that provides web-engine and storage services regarding the Website. You may find more details of Webflow's data processing in the European Union on the following website: EU & Swiss Privacy Policy | Webflow

The Data Controller informs the Data Subject that, in the event of a transfer of personal data to a third country or an international organization, the Data Subject is entitled to be informed of the appropriate guarantees provided for by the GDPR in relation to the transfer. In the case of Webflow Inc., the information on the guarantees regarding the transfer of data to a third country is supported by the Commission Implementing Decision (EU) 2023/1795 on the adequate level of protection of personal data provided by the EU-US Privacy Shield Framework pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (after notification under document C(2023) 4745) („**Data Privacy Framework**"), which corresponds to the conformity decision provided for in Article 45 of the GDPR. Accordingly, the transfer of data to Webflow servers located in the United States of America is not subject to any further authorization.

Formagrid Inc. (registered office: 799 Market St FL 8 San Francisco, CA, 94103-2044 United States): a private company incorporated under the laws of the United States that provides telecommunication services in relation to job applications on the Website. You can find more details of Formagrid's data processing on the following website: Airtable Privacy Policy - Airtable

The Data Controller and Formagrid Inc., the operator of Airtable, have concluded a data processing agreement including the standard contractual clauses on data protection (SCC) set out in Article 46 Section (2) point c) of the GDPR in accordance with the applicable national and European Union regulations in order to provide the appropriate safeguards set out in the GDPR. On this basis, the personal data can be securely transferred to the Data Processor.

Google Ireland Limited (registered office: Gordon House, Barrow Street, Dublin 4; Ireland): a private company incorporated under the laws of Ireland that provides the services of Google Analytics to the Data Controller. You can find more details on the data processing of Google Analytics on the following website: Privacy Policy – Privacy & Terms – Google

For any transfers to third countries, Google LLC (headquarters: 25 Massachusetts Ave NW Ste 900 Washington, DC, 20001-7408 USA), as the parent company of Google Ireland Limited, is part of the list of the Data Privacy Framework compliant organizations, and any transfers to third countries will be in compliance with the applicable rules.

SHL Hungary Vezetéslélektani Managerképző és Alkalmasságvizsgáló Kft. (registered office: 2040 Budaörs, Kossuth L. u. 20.; company registration number: 13-09-118103; tel.: + 36 23 / 703 002; e-mail: support@shl.hu): a company incorporated under Hungarian laws and which provides services relating to conducting personality tests and proficiency tests. You can find more information on the data processor's data processing on the following website: Adatkezelési tájékoztató | SHL Hungary

Microsoft Ireland Operations Limited (registered seat: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland) a private company incorporated under the laws of Ireland which is in a data processing relationship with the Data Controller within the framework of the Microsoft Forms service related to the completion of health declarations. For more information about Microsoft Ireland Operations Limited's data processing, please visit the following link: Microsoft Privacy Statement – Microsoft privacy

For any transfers to third countries, Microsoft Corporation (headquarters: One Microsoft Way, Redmond, Washington 98052, United States), as the parent company of Microsoft Ireland Operations Limited, is part of the list of the Data Privacy Framework compliant organizations, and any transfers to third countries will be in compliance with the applicable rules.

5. DATA SECURITY

5.1. The Data Controller treats the Data Subject's personal data confidentially, therefore Data Controller has adopted the technical and organizational measures necessary to ensure the security of personal data and avoid their accidental or unlawful destruction, loss, alteration, processing or unauthorized access, given the state of the technology, the nature of the stored data and the risks to which they are exposed, whether they come from human action or from the physical or natural environment. The Data Controller selects and operates the IT equipment used to process personal data with respect to the contractual relationship in such a way that the processed data:

(a) is available to authorized persons (availability);

(b) authenticity and authentication are ensured (authenticity of data processing);

(c) integrity can be proven (integrity of data); and

(d) is protected against unauthorized access (confidentiality of data).

6. RIGHTS AND REMEDIES

6.1. The Data Subject has a right to:

- **access the personal data**: Upon the Data Subject's request, the Data Controller supplies information about the Data Subject's data processed by the Data Controller as data controller and/or processed by a data processor on the Data Controller's behalf if any of the conditions stipulated in Article 15 of GDPR is fulfilled.

- **request the rectification of the personal data**: The Data Controller rectifies the Data Subject's personal data if such data is inaccurate or incomplete while the correct personal data is available to the Data Controller.

- **request the erasure of the personal data** ("right to be forgotten"): The Data Controller erases any and all personal data if any of the conditions stipulated in Article 17 of GDPR is fulfilled.

- **restriction of processing**: The Data Subject obtains from the Data Controller the limitation of the data processing if any of the conditions stipulated in Article 18 of GDPR is fulfilled.

- **data portability**: The Data Subject receives the personal data concerning him or her, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format, if the processing is based on a consent or contract and it is carried out by automated means.

- **object:** The Data Subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data on grounds of legitimate interest (Article 6 Section (1) point (f) GDPR). Furthermore, the Data Subject has the right to object to data processing for direct marketing purposes. In the above cases, the Data Subject's personal data may, in principle, no longer be processed on the above basis in accordance with Article 21 GDPR.

6.2. The Data Controller provides information on action taken on the Data Subject's request sent to the contact person specified in Section **Error! Reference source not found.** without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. The Data Controller informs the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the Data Subject makes the request by electronic means, the information will be provided by electronic means where possible, unless otherwise requested by the Data Subject. If the Data Controller does not act on the Data Subject's request, the Data Controller will inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

6.3. Data Subject's right to remedy:

- **filing a complaint with the authority**: Without prejudice to any other administrative or judicial remedy, Data Subject may, in the event of an infringement of his or her rights, file a complaint with the data protection authority (**Data Protection Commission**:

address: 1055 Budapest, Falk Miksa utca 9-11 ;Tel.: +36 1 391 1400, email: ugyfelszolgalat@naih.hu; website: https://www.naih.hu/).

- **filing a complaint with the court**: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, Data Subjects have the right to an effective judicial remedy where he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data in non-compliance with the data protection regulation. The Data Controller is liable for any loss or damage caused by the unlawful processing of the Data Subject's data or by any violation of applicable data-security requirements. The Data Controller will be exempted from such liability if the loss or damage was caused by circumstances beyond its control and outside the scope of data processing. No compensation shall be paid to the extent that the loss or damage was caused by the Data Subject's wilful or grossly negligent conduct.